两方有理数多重集的保密计算

王维琼* 谢 琼 许豪杰 崔 萌
(长安大学理学院 西安 710064)

摘 要：集合的安全多方计算(SMC)在联合数据分析、敏感数据安全查询、数据可信交换等场景有着广泛的应用。该文基于有理数的几何编码，结合保密内积协议，首次提出了有理数域上两方多重集交集和并集的保密计算协议。应用模拟范例证明了协议在半诚实模型下的安全性，分别通过理论分析和仿真测试验证了协议的高效性。与现有协议相比，所设计协议无需给定包含所有集合元素的全集，可以保护集合势的隐私性，且在协议执行过程主要使用乘法运算，达到了信息论安全。

关键词：保密计算；多重集；集合运算；内积协议
中图分类号：TN918; TP309 **文献标识码**：A **文章编号**：1009-5896(2023)05-1722-09
DOI: 10.11999/JEIT220712

Secure Computation of Two-party Multisets with Rational Numbers

WANG Weiqiong XIE Qiong XU Haojie CUI Meng
(*School of Science*, *Chang'an University*, *Xi'an* 710064, *China*)

Abstract: Secure Multiparty Computation (SMC) of sets has wide applications in joint data analysis, secure search over sensitive data, data security exchange. Based on geometric coding of rational numbers and the scalar product protocol, two secure computation protocols for computing the intersection and the union of two multisets with private rational numbers are proposed for the first time. The simulation paradigm is used to prove the privacy- preserving properties of proposed protocols in the semi-honest model, and the protocols' efficiency is verified by theoretical analysis and programming test. Compared with existing protocols, the proposed protocols do not need to specify a universal set, which can protect the privacy of set potential. Moreover, the multiplication operation is mainly used in the implementation of the protocols, which achieves the security of information theory.

Key words: Secure computation; Multiset; Set operation; Scalar product protocol

1 引言

安全多方计算(Secure Multiparty Computation, SMC)最早由Yao[1]提出，是指在互不信任的分布式计算场景下，两方或更多参与者将保密数据作为计算输入，协同进行保密计算，输出计算结果，并保证任何一方都无法得到计算结果之外的其他额外信息。安全多方计算对经济、文化、教育、医疗、互联网等各行各业信息的判断和使用都产生了广泛而深远的影响。

近年来，学者在保密信息比较[2,3]、保密几何计算[4–6]、隐私入侵检测[7]、保密科学计算[8–12]等方面取得了大量研究成果。整数集合的安全多方计算是保密科学计算研究的重要问题之一，学者主要研究了保密判定元素与集合的关系[9,10]、保密计算集合的交集或交集的势[10,11]、保密计算集合的并集[12,13]或并集的势、保密判定集合包含关系[11,14]等问题。文献[8]基于对称加密算法设计了元素与集合关系的保密判定协议。文献[10]借助不经意多项式和同态加密方案设计了元素与集合关系和两方集合交集的保密计算协议。文献[11]结合秘密共享思想，应用多项式性质和离散对数困难问题，用非加密方法设计了计算两方集合交集的保密计算协议。文献[12,13]结合多项式的性质，分别应用翻转罗朗级数和秘密共享，以及全同态加密算法设计了两方集合并集的

收稿日期：2022-06-01；改回日期：2022-08-27；网络出版：2022-09-06
*通信作者： 王维琼 wqwang@chd.edu.cn
基金项目：国家自然科学基金(11901049)，陕西省自然科学基础研究计划(2020JQ-343)，陕西省高校科协青年人才托举计划(20200505)
Foundation Items: The National Natural Science Foundation of China (11901049), The Natural Science Basis Research Plan in Shaanxi Province of China (2020JQ-343), The Young Talent Fund of University Association for Science and Technology in Shaanxi, China (20200505)

保密计算协议。文献[15]应用信息论的方法研究了标准集和多重集的多种运算，但协议要求参与者之间要有安全信道。文献[16]将多重集转化为矩阵，并结合Paillier加密方案设计了两方多重集的交集和并集保密计算协议。

然而许多实际问题如基因序列匹配、行业动向分析、金融风险评估等都可抽象为有理数域上集合的运算问题，因此设计安全高效的有理数域上集合的保密计算协议也具有重要的意义[17–19]。文献[17]基于连分数编码方式和全同态加密算法设计了有理数加密方案。文献[18]提出了对有理数按位编码的思想，结合Paillier加密算法和椭圆曲线同态加密算法分别设计了判定两个或多个有理数相等的保密协议。文献[19]将有理数编码为直线，应用Paillier加密方案设计了有理数域上两方集合运算的保密计算协议。

本文基于文献[19]中几何编码的转化思想，将有理数域上集合的运算问题转化为整数向量内积计算问题，借助保密内积协议分别设计了有理数域上两方多重集的交集和并集的保密计算协议。协议适用于有理数域，对集合元素的数值大小没有任何限制，在执行过程中没有使用公钥加解密算法，达到了信息论安全，而且无需给定包含所有集合元素的全集，可以保护集合势的隐私性。

2　预备知识

2.1　安全性定义

半诚实模型　安全多方计算中常用的模型有半诚实模型和恶意模型两种。半诚实模型下的参与者是诚实且好奇的，他们会严格履行协议内容，但会收集和保留协议中的相关信息，并在完成协议后根据所获得的信息推导其他参与者的私密信息。如果所有参与者都是半诚实的，那么称这样的计算模型为半诚实模型[20]。

模拟范例[21]　设参与者P_1, P_2分别输入保密数据x_1, x_2，并利用协议π保密计算$f(x_1,x_2)=(f_1(x_1,x_2),\ f_2(x_1,x_2))$，其中，$f_i(x_1,x_2)$为参与者$P_i(i=1,2)$得到的输出结果。在协议$\pi$的执行过程中，$P_i$得到的信息序列记为

$$\text{view}_i^{\pi}(x_1,x_2)=(x_i,r_i,m_i^1,m_i^2,\cdots,m_i^t) \tag{1}$$

其中，r_i表示P_i在协议中产生的随机数，$m_i^j(j\in\{1,2,\cdots,t\})$表示$P_i$收到的第$j$条信息。

定义1[20]　在参与者都是半诚实的情况下，如果存在概率多项式时间函数S_1和S_2，使得式(2)和式(3)成立

$$\{S_1(x_1,f_1(x_1,x_2))\}_{x_1,x_2}\overset{c}{\equiv}\{\text{view}_1^{\pi}(x_1,x_2)\}_{x_1,x_2} \tag{2}$$

$$\{S_2(x_2,f_2(x_1,x_2))\}_{x_1,x_2}\overset{c}{\equiv}\{\text{view}_2^{\pi}(x_1,x_2)\}_{x_1,x_2} \tag{3}$$

则称协议π保密地计算了函数f，其中，$\overset{c}{\equiv}$表示计算上不可区分。

2.2　向量内积计算

文献[22]提出了保密内积协议，为了提高协议的执行效率，本文修改了文献[22]设计的协议，针对n维向量的内积计算问题，新协议通过构造$n\times 1$阶矩阵进行保密计算，协议没有应用公钥加解密算法且主要运算为乘法运算。协议具体设计如算法1所示。

算法1　保密内积协议

输入：Alice和Bob分别输入私密向量$\boldsymbol{X}=(x_1,x_2,\cdots,x_n)^{\mathrm{T}}$和$\boldsymbol{Y}=(y_1,y_2,\cdots,y_n)^{\mathrm{T}}$。

输出：Alice输出内积$\boldsymbol{X}\cdot\boldsymbol{Y}=\sum_{i=1}^{n}x_iy_i$。

(1)Alice和Bob共同生成一个$n\times 1$阶的矩阵$\boldsymbol{P}$。

(2)Alice进行如下操作：

(a)随机生成一个1维向量$\boldsymbol{R}=(r)$。

(b)计算$n\times 1$阶矩阵$\boldsymbol{X'}$：$\boldsymbol{X'}=\boldsymbol{PR}$。

(c)计算$\boldsymbol{X''}=\boldsymbol{X'}+\boldsymbol{X}$，并将$\boldsymbol{X''}$发送给Bob。

(3)Bob进行如下操作：

(a)计算内积Z'：$Z'=\boldsymbol{X''}\cdot\boldsymbol{Y}=\sum_{i=1}^{n}x_i''y_i$。

(b)计算1阶矩阵$\boldsymbol{Y'}$：$\boldsymbol{Y'}=\boldsymbol{P}^{\mathrm{T}}\boldsymbol{Y}$。

(c)将Z'和$\boldsymbol{Y'}$发送给Alice。

(4)Alice进行如下操作：

(a)计算减法因子Z''：$Z''=\boldsymbol{R}\cdot\boldsymbol{Y'}=r\sum_{i=1}^{n}p_iy_i$。

(b)计算内积Z：$Z=Z'-Z''$。最后输出内积$Z=\boldsymbol{X}\cdot\boldsymbol{Y}$。

2.3　三角形面积公式

在平面直角坐标系中，假设三角形的3个顶点$p_1(x_1,y_1)$, $p_2(x_2,y_2)$和$p_3(x_3,y_3)$按逆时针顺序排列，则三角形面积$S_{\triangle p_1p_2p_3}$可表示为

$$\begin{aligned}S_{\triangle p_1p_2p_3}=&\frac{1}{2}[y_1(x_3-x_2)+x_1(y_2-y_3)\\&+x_2y_3-x_3y_2]\end{aligned} \tag{4}$$

并且$S_{\triangle p_1p_2p_3}=0$当且仅当$p_1,p_2,p_3$ 3点共线。

3　有理数域上两方多重集的保密计算

3.1　编码方式

由于平面直角坐标系中经过坐标原点且斜率为k的直线上任意不为原点的一点(x,y)都满足$k=y/x$，因此有理数k可转化为经过坐标原点且斜率为k的

直线上任意不为原点的坐标点(x,y)，下文中任意选取的坐标点均不包括坐标原点。

3.2 有理数域上元素与集合关系的判定

设Alice拥有私密的有理数集合$U=\{u_1,u_2,\cdots,u_n\}$，Bob拥有私密的有理数v，两人保密判断有理数v是否属于有理数集U，即判断是否存在$u_j\in U$ $(j\in\{1,2,\cdots,n\})$与v相等。

Alice将$u_j\in U(j=1,2,\cdots,n)$转化为斜率为u_j的直线上的整数点(横坐标和纵坐标都为整数的点)，并保证每个元素u_j都至少对应1个整数点以便隐藏集合的势，不妨设共得到了$l(l\geq n)$个不同的整数点$p_i(x_i,y_i)$ $(i=1,2,\cdots,l)$。Bob将v转化为斜率为v的直线L_0上不同的整数点$q_1(x_{01},y_{01})$,$q_2(x_{02},y_{02})$，则p_i,q_1,q_2 3点构成的$\triangle p_iq_1q_2$面积为

$$S_{\triangle p_iq_1q_2}=\frac{1}{2}|y_i(x_{02}-x_{01})+x_i(y_{01}-y_{02})+x_{01}y_{02}-x_{02}y_{01}| \tag{5}$$

又因为q_1和q_2是在直线L_0上的任意两点，所以$x_{01}y_{02}=x_{02}y_{01}$，因此，式(5)可转化为

$$\begin{aligned}S_{\triangle p_iq_1q_2}&=\frac{1}{2}|y_i(x_{02}-x_{01})+x_i(y_{01}-y_{02})|\\&=\frac{1}{2}|ay_i+bx_i|\end{aligned} \tag{6}$$

如果$v\in U$，那么集合U中存在$u_j(j\in\{1,2,\cdots,n\})$使得$u_j=v$，即$v\in U$当且仅当存在$t\in\{1,2,\cdots,l\}$使得$S_{\triangle p_tq_1q_2}=0$，从而$p_i(i=1,2,\cdots,l)$和$q_1,q_2$构成的$l$个三角形面积乘积为0。

为了保密判断v是否属于集合U，且在v属于集合U的情况下，不泄露v与集合U中的哪个元素相等，记$S=\prod_{i=1}^{l}(ay_i+bx_i)=a^lc_l+a^{l-1}bc_{l-1}+\cdots+ab^{l-1}c_1+b^lc_0$，定义向量$\boldsymbol{A}$和$\boldsymbol{C}$

$$\boldsymbol{A}=(a^l,a^{l-1}b,\cdots,ab^{l-1},b^l),\boldsymbol{C}=(c_l,c_{l-1},\cdots,c_1,c_0) \tag{7}$$

其中，$a=x_{02}-x_{01}$, $b=y_{01}-y_{02}$, $c_{l-k}=\sum_{i_1,i_2,\cdots,i_k\in\{1,2,\cdots,l\}}(x_{i_1}x_{i_2}\cdots x_{i_k}\prod_{j\neq i_1,i_2,\cdots,i_k}y_j)$,$0\leq k\leq l$。因此

$$v\in U\Leftrightarrow S=\prod_{i=1}^{l}(ay_i+bx_i)=0\Leftrightarrow\boldsymbol{A}\cdot\boldsymbol{C}=0 \tag{8}$$

3.3 有理数域上两方多重集交集的保密计算

3.3.1 问题描述

假设Alice和Bob分别拥有私密有理数多重集U和V，且多重集U和V中元素最大重数不超过d，双方希望保密计算$U\cap V$。

记$U=\{<u_{11},u_{21}>,<u_{12},u_{22}>,\cdots,<u_{1n},u_{2n}>\}$，$V=\{<v_{11},v_{21}>,<v_{12},v_{22}>,\cdots,<v_{1m}\cdot v_{2m}>\}$，其中，$u_{1i},v_{1j}$分别为有理数多重集$U,V$中的元素；$u_{2i},v_{2j}$分别为元素$u_{1i},v_{1j}$出现的次数，满足$0<u_{2i}\leq d,0<v_{2j}\leq d$, $i=1,2,\cdots,n,j=1,2,\cdots,m$。

计算原理1 Alice和Bob分别根据私密多重集U,V构造标准集U_1和V_1，其中，$U_1=\{u_{11},u_{12},\cdots,u_{1n}\}$,$V_1=\{v_{11},v_{12},\cdots,v_{1m}\}$，将保密计算多重集交集$U\cap V$的问题分成两步：

(1)保密计算标准集交集$X_1=U_1\cap V_1=\{x_{11},x_{12},\cdots,x_{1k}\}$。

Alice和Bob协商正整数l，满足$l>\max\{n,m\}$。Alice将U_1中元素u_{1i}转化为斜率为u_{1i}的直线上的任意整数点，满足每个元素至少对应1个整数点，不妨设共得到l个不同的整数点，并根据式(7)构造U_1对应的向量$\boldsymbol{C}=(c_l,c_{l-1},\cdots,c_1,c_0)^{\mathrm{T}}$。Bob在斜率为$v_{1j}(j=1,2,\cdots,m)$的直线上任意选择两个不同整数点，根据式(7)构造$v_{1j}$对应的向量$\boldsymbol{A}_j=(a_j{}^l,a_j{}^{l-1}b_j,\cdots,a_jb_j{}^{l-1},b_j{}^l)^{\mathrm{T}}$，则$v_{1j}\in U_1\Leftrightarrow\boldsymbol{A}_j\cdot\boldsymbol{C}=0$，计算得到标准集交集$X_1=U_1\cap V_1$。

(2)计算X_1中元素$x_{1i}(i=1,2,\cdots,k)$的重数，设x_{1i}在U,V中的重数分别为p_i,q_i，则在交集$U\cap V$中x_{1i}的重数为$x_{2i}=\min\{p_i,q_i\}$。

Alice和Bob通过步骤(1)得到标准集交集$X_1=\{x_{11},x_{12},\cdots,x_{1k}\}$，两人根据$x_{1i}(i=1,2,\cdots,k)$在$U$和$V$的重数$p_i,q_i$分别构造$d$维向量$\boldsymbol{S}_i=(s_{i1},s_{i2},\cdots,s_{id})^{\mathrm{T}}$和$\boldsymbol{T}_i=(t_{i1},t_{i2},\cdots,t_{id})^{\mathrm{T}}$。当$0<j\leq p_i$时，$s_{ij}=1$；当$p_i<j\leq d$时，$s_{ij}=0$；当$0<j\leq q_i$时，$t_{ij}=1$；当$q_i<j\leq d$时，$t_{ij}=0$。则$x_{1i}$的重数$x_{2i}=\boldsymbol{S}_i\cdot\boldsymbol{T}_i=\min\{p_i,q_i\}$。

通过上述计算得到有理数域上两方多重集交集$X=U\cap V=\{<x_{11},x_{21}>,<x_{12},x_{22}>,\cdots,<x_{1k},x_{2k}>\}$。

由于Alice和Bob双方都知道向量$\boldsymbol{S}_i,\boldsymbol{T}_i$是由0, 1构成的，在交集元素重数的计算过程如果直接调用保密内积协议计算内积$\boldsymbol{S}_i\cdot\boldsymbol{T}_i$，则Bob在交集中的元素重数会被泄露。为了解决上述问题，提出下述命题：

命题1 已知n维向量$\boldsymbol{X}$和$\boldsymbol{Y}$，随机生成n维向量$\boldsymbol{X}_1,\boldsymbol{Y}_1$，计算向量$\boldsymbol{X}_2,\boldsymbol{Y}_2$，其中，$\boldsymbol{X}_2=\boldsymbol{X}-\boldsymbol{X}_1$,$\boldsymbol{Y}_2=\boldsymbol{Y}-\boldsymbol{Y}_1$，则内积$\boldsymbol{X}\cdot\boldsymbol{Y}=\boldsymbol{X}_1\cdot\boldsymbol{Y}_1+\boldsymbol{X}_1\cdot\boldsymbol{Y}_2+\boldsymbol{X}_2\cdot\boldsymbol{Y}_1+\boldsymbol{X}_2\cdot\boldsymbol{Y}_2$。

3.3.2 协议设计

详细设计内容见协议1。

3.3.3 正确性分析

对协议1的正确性，需要证明计算得到的标准集交集X_1与X_1中元素的重数集合X_2均正确。

协议1 有理数域上两方多重集交集的保密计算

输入：Alice和Bob分别输入有理数多重集$U=\{<u_{11},u_{21}>,<u_{12},u_{22}>,\cdots,<u_{1n},u_{2n}>\}$和$V=\{<v_{11},v_{21}>,<v_{12},v_{22}>,\cdots,<v_{1m}\cdot v_{2m}>\}$。

输出：交集$U\cap V$。

准备：Alice和Bob根据计算原理1构造标准集U_1,V_1，并协商正整数l，合作生成$(l+1)\times 1$阶矩阵$\boldsymbol{P}_1$。Alice将U_1中元素转化为对应直线上的整数点，保证每个元素至少对应1个整数点，设共得到l个整数点，根据式(7)构造标准集U_1对应的向量$\boldsymbol{C}=(c_l,c_{l-1},\cdots,c_1,c_0)^{\mathrm{T}}$。Bob将$v_{1j}(j=1,2,\cdots,m)$转化为对应直线上的任意两个整数点，构造$v_{1j}$对应的向量$\boldsymbol{A}_j=({a_j}^l,{a_j}^{l-1}b_j,\cdots,a_j{b_j}^{l-1},{b_j}^l)^{\mathrm{T}}$。

对$j=1,2,\cdots,l$，Alice和Bob执行如下步骤：

(1)Alice进行如下操作：

(a)随机生成1维向量$\boldsymbol{R}_j=(r_j)$。

(b)生成对应的$(l+1)\times 1$阶矩阵$\boldsymbol{C}'_j$：$\boldsymbol{C}'_j=\boldsymbol{P}_1\boldsymbol{R}_j$。

(c)计算$\boldsymbol{C}''_j=\boldsymbol{C}'_j+\boldsymbol{C}$，并将所有的$\boldsymbol{C}''_j$发送给Bob。

(2)Bob进行如下操作：

(a)对$j=1,2,\cdots,m$计算内积Z'_j：$Z'_j=\boldsymbol{A}_j\cdot\boldsymbol{C}''_j$；对$j=m+1,m+2,\cdots,l$随机生成$l+1$维向量$\boldsymbol{A}_j$，并计算内积$Z'_j=\boldsymbol{A}_j\cdot\boldsymbol{C}''_j$。

(b)生成对应的1阶矩阵$\boldsymbol{A}'_j$：$\boldsymbol{A}'_j=\boldsymbol{P}_1^{\mathrm{T}}\boldsymbol{A}_j$。

(c)将Z'_j和$\boldsymbol{A}'_j$发送给Alice。

(3)Alice进行如下操作：

(a)生成减法因子Z''_j：$Z''_j=\boldsymbol{R}_j\cdot\boldsymbol{A}'_j$。

(b)计算内积Z_j：$Z_j=Z'_j-Z''_j=\boldsymbol{A}_j\cdot\boldsymbol{C}$。如果$Z_j=0$，令$e_j=1$；否则$e_j=0$，得到向量$\boldsymbol{E}=(e_1,e_2,\cdots,e_l)$，将向量$\boldsymbol{E}$发送给Bob。

(4)Bob选取向量$\boldsymbol{E}$中前m个分量中1所在位置对应的元素v_{1j}构成集合X_1，将集合X_1中的元素进行随机置换后输出集合$X_1=U_1\cap V_1=\{x_{11},x_{12},\cdots,x_{1k}\}$。

(5)Alice和Bob按照计算原理1根据$x_{1i}(i=1,2,\cdots,k)$在U,V中的重数p_i,q_i构造d维向量$\boldsymbol{S}_i=(s_{i1},s_{i2},\cdots,s_{id})^{\mathrm{T}}$和$\boldsymbol{T}_i=(t_{i1},t_{i2},\cdots,t_{id})^{\mathrm{T}}$，两人分别随机生成$d$维向量$\boldsymbol{S}_i^1,\boldsymbol{T}_i^1$，计算$\boldsymbol{S}_i^2$和$\boldsymbol{T}_i^2$，其中，$\boldsymbol{S}_i^2=\boldsymbol{S}_i-\boldsymbol{S}_i^1,\boldsymbol{T}_i^2=\boldsymbol{T}_i-\boldsymbol{T}_i^1$，并合作生成$d\times 1$阶矩阵$\boldsymbol{P}_2$。

对$i=1,2,\cdots,k$，Alice和Bob执行如下步骤：

(6)Alice进行如下操作：

(a)生成4个1维向量$\boldsymbol{R}_i^{ab}=({r_i}^{ab})$，$a=1,2,b=1,2$。

(b)对应计算$d\times 1$阶矩阵$\boldsymbol{S}_i'^{ab}=\boldsymbol{P}_2\boldsymbol{R}_i^{ab}$。

(c)计算$\boldsymbol{S}_i''^{ab}=\boldsymbol{S}_i'^{ab}+\boldsymbol{S}_i^a$，并将所有的$\boldsymbol{S}_i''^{ab}$发送给Bob。

(7)Bob进行如下操作：

(a)计算内积${W'}_i^{ab}=\boldsymbol{S}_i''^{ab}\cdot\boldsymbol{T}_i^b$。

(b)计算1阶矩阵$\boldsymbol{T}_i'^{ab}=\boldsymbol{P}_2^{\mathrm{T}}\boldsymbol{T}_i^b$。

(c)将${W'}_i^{ab}$和${\boldsymbol{T}'}_i^{ab}$发送给Alice。

(8)Alice进行如下操作：

(a)计算$W_i''^{ab}=\boldsymbol{T}_i'^{ab}\cdot\boldsymbol{R}_i^{ab}$。

(b)计算内积$W_i^{ab}=W'ab_i^-W_i''^{ab}=\boldsymbol{S}_i^a\cdot\boldsymbol{T}_i^b$。

(c)令$x_{2i}=W_i=W_i^{11}+W_i^{12}+W_i^{21}+W_i^{22}=\boldsymbol{S}_i\cdot\boldsymbol{T}_i$，得到集合$X_2=\{x_{21},x_{22},\cdots,x_{2k}\}$。

(9)输出两方多重集交集$X=U\cap V=\{<x_{11},x_{21}>,<x_{12},x_{22}>,\cdots,<x_{1k},x_{2k}>\}$。

标准集交集计算的正确性意味着对Alice和Bob根据任意输入的多重集U,V构造的标准集U_1和V_1，协议能正确地输出$U_1\cap V_1$。

第(1)步，对$j=1,2,\cdots,l$，Alice计算

$$\begin{aligned}\boldsymbol{C}'_j&=\boldsymbol{P}_1\boldsymbol{R}_j=\begin{bmatrix}p_1^1 & p_2^1 & \cdots & p_{l+1}^1\end{bmatrix}^{\mathrm{T}}[r_j]\\&=\begin{bmatrix}r_jp_1^1 & r_jp_2^1 & \cdots & r_jp_{l+1}^1\end{bmatrix}^{\mathrm{T}}\end{aligned}\tag{9}$$

$$\begin{aligned}\boldsymbol{C}''_j&=\boldsymbol{C}+\boldsymbol{C}'_j\\&=\begin{bmatrix}c_l+r_jp_1^1 & c_{l-1}+r_jp_2^1 & \cdots & c_0+r_jp_{l+1}^1\end{bmatrix}^{\mathrm{T}}\end{aligned}\tag{10}$$

第(2)步，Bob计算

$$Z'_j=\boldsymbol{A}_j\cdot\boldsymbol{C}''_j=\sum_{i=1}^{l+1}a_j^{(l+1)-i}b_j^{i-1}(c_{(l+1)-i}+r_jp_i^1)\tag{11}$$

$$\begin{aligned}\boldsymbol{A}'_j=&\boldsymbol{P}_1^{\mathrm{T}}\boldsymbol{A}_j=\begin{bmatrix}p_1^1 & p_2^1 & \cdots & p_{l+1}^1\end{bmatrix}\\&\cdot\begin{bmatrix}a_j^l & a_j^{l-1}b_j & \cdots & b_j^l\end{bmatrix}^{\mathrm{T}}=\left[\sum_{i=1}^{l+1}p_i^1a_j^{(l+1)-i}b_j^{i-1}\right]\end{aligned}\tag{12}$$

第(3)步，Alice计算

$$Z_j'' = \boldsymbol{R}_j \cdot \boldsymbol{A}_j' = \sum_{i=1}^{l+1} r_j p_i^1 a_j^{(l+1)-i} b_j^{i-1} \tag{13}$$

$$\begin{aligned} Z_j =& Z_j' - Z_j'' = \sum_{i=1}^{l+1} a_j^{(l+1)-i} b_j^{i-1} (c_{(l+1)-i} + r_j p_i^1) \\ & - \sum_{i=1}^{l+1} r_j p_i^1 a_j^{(l+1)-i} b_j^{i-1} \\ =& \sum_{i=1}^{l+1} a_j^{(l+1)-i} b_j^{i-1} c_{(l+1)-i} = a_j^l c_l + a_j^{l-1} b_j c_{l-1} \\ & + \cdots + a_j b_j^{l-1} c_1 + b_j^l c_0 \\ =& \boldsymbol{A}_j \cdot \boldsymbol{C} \end{aligned} \tag{14}$$

因此，对$j = 1, 2, \cdots, l$均有$Z_j = \boldsymbol{A}_j \cdot \boldsymbol{C}$。如果存在$j \in \{1, 2, \cdots, m\}$，使得$Z_j = \boldsymbol{A}_j \cdot \boldsymbol{C} = 0$，那么$v_{1j} \in U_1$，所以$v_{1j} \in U_1 \cap V_1$。故在$\boldsymbol{E} = (e_1, e_2, \cdots, e_l)$的分量中，如果$j \in \{1, 2, \cdots, m\}$且$e_j = 1$，那么$v_{1j} \in U_1 \cap V_1$，即所有满足条件的$v_{1j}$构成了$U_1$和$V_1$的交集$X_1$。

下面说明调用保密内积协议计算的标准集交集中元素重数是正确的。Alice和Bob根据标准集交集中元素$x_{1i}(i = 1, 2, \cdots, k)$在集合$U$和$V$中的重数$p_i, q_i$构造$d$维向量$\boldsymbol{S}_i$和$\boldsymbol{T}_i$，得到

$$\boldsymbol{S}_i = \left(\underbrace{1, 1, \cdots, 1}_{p_i\text{个}1}, 0, \cdots, 0 \right)^{\mathrm{T}}, \boldsymbol{T}_i = \left(\underbrace{1, 1, \cdots, 1}_{q_i\text{个}1}, 0, \cdots, 0 \right)^{\mathrm{T}} \tag{15}$$

其中，$0 < p_i \le d$, $0 < q_i \le d$。两人随机生成向量$\boldsymbol{S}_i^1, \boldsymbol{T}_i^1$，计算$\boldsymbol{S}_i^2$和$\boldsymbol{T}_i^2$，其中，$\boldsymbol{S}_i^2 = \boldsymbol{S}_i - \boldsymbol{S}_i^1$, $\boldsymbol{T}_i^2 = \boldsymbol{T}_i - \boldsymbol{T}_i^1$，由命题1计算得内积$\boldsymbol{S}_i \cdot \boldsymbol{T}_i$，元素$x_{1i}$的重数$x_{2i} = \boldsymbol{S}_i \cdot \boldsymbol{T}_i = \min\{p_i, q_i\}$。因此，协议1是正确的。

3.3.4 安全性分析

协议1的设计主要分为标准集交集的计算和交集元素重数的计算两部分。在计算标准集交集的过程中，Alice和Bob共同商议得到正整数l，Alice在集合U_1中n个元素对应的直线上随机选取$l(l > n)$个整数点，这样不仅保密了标准集U_1的势，而且不影响协议输出正确结果。协议的(1)～(3)步严格遵循保密内积协议，其安全性可由保密内积协议的安全性来保证。最后，Bob收到Alice发送的向量$\boldsymbol{E}$，并将其前m个分量中1所在位置对应的v_{1j}构成集合X_1，将集合X_1中的元素随机置换后输出结果。由于m是Bob的保密数据，输出的交集不会泄露Bob集合的其他隐私数据包括标准集的势，所以标准集交集的计算过程是安全的。

在交集元素重数计算的过程中，Alice和Bob根据$\boldsymbol{S}_i, \boldsymbol{T}_i$构造新向量$\boldsymbol{S}_i^1, \boldsymbol{S}_i^2$和$\boldsymbol{T}_i^1, \boldsymbol{T}_i^2$。因为新向量的构造只需满足$\boldsymbol{S}_i = \boldsymbol{S}_i^1 + \boldsymbol{S}_i^2$和$\boldsymbol{T}_i = \boldsymbol{T}_i^1 + \boldsymbol{T}_i^2$，且新向量的各分量仅为参与者自己所知，所以执行协议计算内积的过程中双方集合均没有隐私信息的泄露。下面通过模拟范例的方法证明协议1在半诚实模型下是安全的。

定理1 在半诚实模型下协议1是安全的。

证明 通过构造满足式(2)(或式(3))的模拟器S_1(或S_2)来证明定理的正确性。

假设模拟器S_1接受输入$(U, f_1(U, V))$，按下述方式运行：

(1) S_1任意选择集合$V' = \{< v_{11}', v_{21}' >, < v_{12}', v_{22}' >, \cdots, < v_{1m'}', v_{2m'}' >\}$，满足$f_1(U, V') = f_1(U, V)$，构造标准集$V_1' = \{v_{11}', v_{12}', \cdots, v_{1m'}'\}$，对$j = 1, 2, \cdots, m'$根据式(7)构造$V_1'$中各元素对应的向量$\hat{\boldsymbol{A}}_j = (\hat{a}_j^l, \hat{a}_j^{l-1}\hat{b}_j, \cdots, \hat{a}_j\hat{b}_j^{l-1}, \hat{b}_j^l)^{\mathrm{T}}$，对$j = m', m'+1, \cdots, l$任意生成$l+1$维向量$\hat{\boldsymbol{A}}_j$。

(2) S_1计算内积$\hat{Z}_j' = \hat{\boldsymbol{A}}_j' \cdot \boldsymbol{C}_j''$和矩阵$\hat{\boldsymbol{A}}_j' = \boldsymbol{P}_1^{\mathrm{T}} \hat{\boldsymbol{A}}_j$。

(3) S_1计算$\hat{Z}_j'' = \boldsymbol{R}_j \cdot \hat{\boldsymbol{A}}_j'$和内积$\hat{Z}_j = \hat{Z}_j' - \hat{Z}_j'' = \hat{\boldsymbol{A}}_j \cdot \boldsymbol{C}$。如果$\hat{Z}_j = 0$，令$\hat{e}_j = 1$；否则$\hat{e}_j = 0$，得到$l$维向量$\hat{\boldsymbol{E}} = (\hat{e}_1, \hat{e}_2, \cdots, \hat{e}_l)$。

(4) S_1构造交集X_1中各元素重数对应的向量$\hat{\boldsymbol{T}}_i$，并随机构造向量$\hat{\boldsymbol{T}}_i^1, \hat{\boldsymbol{T}}_i^2 (i = 1, 2, \cdots, k)$。

(5) S_1计算内积$\hat{W}_i'^{ab} = \boldsymbol{S}_i''^{ab} \cdot \hat{\boldsymbol{T}}_i^b$和矩阵$\hat{\boldsymbol{T}}_i'^{ab} = \boldsymbol{P}_2^{\mathrm{T}} \hat{\boldsymbol{T}}_i^b (a = 1, 2, b = 1, 2)$。

(6) S_1计算$\hat{W}_i''^{ab} = \hat{\boldsymbol{T}}_i'^{ab} \cdot \boldsymbol{R}_i^{ab}$和内积$\hat{W}_i^{ab} = \hat{W}_i'^{ab} - \hat{W}_i''^{ab} = \boldsymbol{S}_i^a \cdot \hat{\boldsymbol{T}}_i^b$。

在协议执行过程中，$\mathrm{view}_1^{\pi}(U, V) = (U, Z_j', \boldsymbol{A}_j', W_i'^{ab}, \boldsymbol{T}_i'^{ab}, f_1(U, V))$。

S_1在模拟过程中产生的信息序列为：$S_1(U, f_1(U, V)) = (U, \hat{Z}_j', \hat{\boldsymbol{A}}_j', \hat{W}_i'^{ab}, \hat{\boldsymbol{T}}_i'^{ab}, f_1(U, V'))$。

由于向量$\hat{\boldsymbol{A}}_j, \hat{\boldsymbol{T}}_i'^{ab}$构造的任意性，所以对Alice来讲，在计算过程中，有$Z_j' \overset{c}{\equiv} \hat{Z}_j'$，$\boldsymbol{A}_j' \overset{c}{\equiv} \hat{\boldsymbol{A}}_j'$，$W_i'^{ab} \overset{c}{\equiv} \hat{W}_i'^{ab}$，$\boldsymbol{T}_i'^{ab} \overset{c}{\equiv} \hat{\boldsymbol{T}}_i'^{ab}$，其中，$j = 1, 2, \cdots, l$, $i = 1, 2, \cdots, k, a = 1, 2, b = 1, 2$，因此

$$\begin{aligned} & \{S_1(U, f_1(U, V))\}_{u_{1i}, v_{1j} \in Q, u_{2i}, v_{2j} \in Z^+} \overset{c}{\equiv} \\ & \quad \{\mathrm{view}_1^{\pi}(U, V)\}_{u_{1i}, v_{1j} \in Q, u_{2i}, v_{2j} \in Z^+} \end{aligned} \tag{16}$$

其中，$i = 1, 2, \cdots, n, j = 1, 2, \cdots, m$。

模拟器S_2接受输入$(V, f_2(U, V))$，按下述方式运行：

(1) S_2任意选择集合$U' = \{< u_{11}', u_{21}' >, < u_{12}', u_{22}' >, \cdots, < u_{1n'}', u_{2n'}' >\}$，满足$f_2(U', V) = f_2(U, V)$，构造标准集$U_1' = \{u_{11}', u_{12}', \cdots, u_{1n'}'\}$，并根据式(7)构造$U_1'$对应的向量$\hat{\boldsymbol{C}} = (\hat{c}_l, \hat{c}_{l-1}, \cdots, \hat{c}_1, \hat{c}_0)^{\mathrm{T}}$。

(2) S_2随机生成$\hat{\boldsymbol{R}}_j = (\hat{r}_j)$，并计算$\hat{\boldsymbol{C}}_j' = \boldsymbol{P}\hat{\boldsymbol{R}}_j$和

$\hat{\boldsymbol{C}}_j'' = \hat{\boldsymbol{C}}_j' + \hat{\mathrm{C}}$, $j = 1, 2, \cdots, l$。

(3)S_2计算$\hat{Z}_j' = \boldsymbol{A}_j \cdot \hat{\boldsymbol{C}}_j''$。

(4)S_2计算$\hat{Z}_j'' = \hat{\boldsymbol{R}}_j \cdot \boldsymbol{A}_j'$和内积$\hat{Z}_j = \hat{Z}_j' - \hat{Z}_j'' = \boldsymbol{A}_j \cdot \hat{\boldsymbol{C}}$。如果$\hat{Z}_j = 0$，令$\hat{e}_j = 1$；否则$\hat{e}_j = 0$，得到$l$维向量$\hat{\boldsymbol{E}} = (\hat{e}_1, \hat{e}_2, \cdots, \hat{e}_l)$。

(5)S_2构造交集X_1中各元素重数对应的向量$\hat{\boldsymbol{S}}_i$，并随机构造向量$\hat{\boldsymbol{S}}_i^1, \hat{\boldsymbol{S}}_i^2 (i = 1, 2, \cdots, k)$。

(6)S_2生成向量$\hat{\boldsymbol{R}}_i^{ab} = (\hat{r}_i^{ab})$，计算$\hat{\boldsymbol{S}}_i'^{ab} = \boldsymbol{P}_2 \hat{\boldsymbol{R}}_i^{ab}$和$\hat{\boldsymbol{S}}_i''^{ab} = \hat{\boldsymbol{S}}_i'^{ab} + \hat{\boldsymbol{S}}_i^a$ $(a = 1, 2, b = 1, 2)$。

(7)S_2计算$\hat{W}_i'^{ab} = \hat{\boldsymbol{S}}_i''^{ab} \cdot \boldsymbol{T}_i^b$。

(8)S_2计算$\hat{W}_i''^{ab} = \boldsymbol{T'}_i^{ab} \cdot \hat{\boldsymbol{R}}_i^{ab}$和内积$\hat{W}_i^{ab} = \hat{W}_i'^{ab} - \hat{W}_i''^{ab} = \boldsymbol{S}_i^a \cdot \hat{\boldsymbol{T}}_i^b$。

在协议执行过程中，$\mathrm{view}_2^{\pi}(U, V) = (V, \boldsymbol{C}_j'', \boldsymbol{E}, \boldsymbol{S}_i''^{ab}, f_2(U, V))$。

S_2在模拟过程中产生的信息序列为：$S_2(V, f_2(U, V)) = (V, \hat{\boldsymbol{C}}_j'', \hat{\boldsymbol{E}}, \hat{\boldsymbol{S}}_i''^{ab}, f_2(U', V))$。

由于生成向量$\hat{\boldsymbol{R}}_j$, $\hat{\boldsymbol{R}}_i^{ab}$的任意性，所以对Bob来讲，在计算过程中，有$\boldsymbol{C}_j'' \overset{c}{\equiv} \hat{\boldsymbol{C}}_j''$, $\boldsymbol{E} \overset{c}{\equiv} \hat{\boldsymbol{E}}$, $\boldsymbol{S}_i''^{ab} \overset{c}{\equiv} \hat{\boldsymbol{S}}_i''^{ab}$，其中，$j = 1, 2, \cdots, l, i = 1, 2, \cdots, k, a = 1, 2, b = 1, 2$，因此

$$\{S_2(V, f_2(U, V))\}_{u_{1i}, v_{1j} \in Q, u_{2i}, v_{2j} \in Z^+} \overset{c}{\equiv} \{\mathrm{view}_2^{\pi}(U, V)\}_{u_{1i}, v_{1j} \in Q, u_{2i}, v_{2j} \in Z^+} \tag{17}$$

其中，$i = 1, 2, \cdots, n, j = 1, 2, \cdots, m$。

3.4 有理数域上两方多重集并集的保密计算

3.4.1 问题描述

Alice和Bob分别拥有有理数域上的多重集U和V，且多重集U和V中集合元素最大重数不超过d，双方希望保密计算$U \cup V$且不泄露集合的其他信息。

计算原理2：Alice和Bob分别根据私密多重集U, V构造标准集U_1和V_1，其中，$U_1 = \{u_{11}, u_{12}, \cdots, u_{1n}\}$, $V_1 = \{v_{11}, v_{12}, \cdots, v_{1m}\}$，将保密计算多重集并集$U \cup V$的问题分成两步：

(1)保密计算标准集并集$Y_1 = U_1 \cup V_1 = \{y_{11}, y_{12}, \cdots, y_{1h}\}$。

因为$U_1 \cup V_1 = U_1 \cup (V_1 \backslash U_1)$，所以Alice和Bob将标准集$V_1$中不属于$U_1$的元素构成的集合与$U_1$取并集就可得到两集合的并集$Y_1$。

(2)计算Y_1中元素$y_{1i} (i = 1, 2, \cdots, h)$的重数，设$y_{1i}$在$U, V$中的重数分别为$p_i, q_i$，则在并集$U \cup V$中$y_{1i}$的重数为$y_{2i} = \max\{p_i, q_i\}$。

Alice和Bob通过步骤(1)得到标准集并集$Y_1 = \{y_{11}, y_{12}, \cdots, y_{1h}\}$，两人根据$y_{1i} (i = 1, 2, \cdots, h)$在$U$和$V$中的重数$p_i, q_i$分别构造$d$维向量$\boldsymbol{S}_i = (s_{i1}, s_{i2}, \cdots, s_{id})^{\mathrm{T}}$和$\boldsymbol{T}_i = (t_{i1}, t_{i2}, \cdots, t_{id})^{\mathrm{T}}$。当$0 < j \le p_i$时，$s_{ij} = 0$；当$p_i < j \le d$时，$s_{ij} = 1$；当$0 < j \le q_i$时，$t_{ij} = 0$；当$q_i < j \le d$时，$t_{ij} = 1$。则$y_{1i}$的重数为$y_{2i} = d - \boldsymbol{S}_i \cdot \boldsymbol{T}_i = \max\{p_i, q_i\}$。

详细设计内容见协议2。

3.4.2 正确性分析

对协议2的正确性，需要证明计算得到的标准集并集Y_1和Y_1中元素的重数集合Y_2均正确。

协议在第(3)步计算内积$Z_j (j = 1, 2, \cdots, l)$，得到$l$维向量$\boldsymbol{E} = (e_1, e_2, \cdots, e_l)$。对$j = 1, 2, \cdots, m$，如果$e_j = 1$，那么$v_{1j} \in U_1$，否则$v_j \notin U_1$，则$e_j = 0 (j \in \{1, 2, \cdots, m\})$所在位置对应的元素$v_{1j}$构成了$V_1 \backslash U_1$。Alice随机选取整数$r$，随机将$\boldsymbol{E}$中的$r$个1变为0，得到向量$\boldsymbol{E'}$。Bob选取$\boldsymbol{E'}$中的前$m$个分量中0所在位置对应的$v_{1j}$构成集合$H$，$H$满足$V_1 \backslash U_1 \subseteq H$，所以$Y_1 = U_1 \cup H = U_1 \cup V_1$，协议2计算得到的$U_1, V_1$的并集$Y_1$是正确的。

下面说明调用保密内积协议计算的标准集并集中y_{1i}的重数y_{2i}是正确的。Alice和Bob根据标准集并集中元素$y_{1i} (i = 1, 2, \cdots, h)$在集合$U, V$中的重数$p_i$, q_i构造d维向量$\boldsymbol{S}_i$和$\boldsymbol{T}_i$，得到

协议2 有理数域上两方多重集并集的保密计算

协议2保持协议1中第(1)和第(2)步不变，对后续步骤做如下修改，输出有理数域上两方多重集并集$U \cup V$。

(3)Alice进行如下操作：

(a)生成减法因子Z_j''：$Z_j'' = \boldsymbol{R}_j \cdot \boldsymbol{A}_j'$。

(b)计算内积Z_j：$Z_j = Z_j' - Z_j'' = \boldsymbol{A}_j \cdot \boldsymbol{C}$。如果$Z_j = 0$，令$e_j = 1$；否则$e_j = 0$，得到$l$维向量$\boldsymbol{E} = (e_1, e_2, \cdots, e_l)$。

(c)随机选取整数r，满足$0 \le r < \sum_{i=1}^{l} e_i$，在$\boldsymbol{E}$的分量中选取$r$个1变为0，得到新的向量$\boldsymbol{E'}$，把$\boldsymbol{E'}$发送给Bob。

(4)Bob选取$\boldsymbol{E'}$中的前m个分量中0所在位置对应的v_{1j}构成集合H，将H中元素随机置换后发送给Alice。

(5)Alice输出$Y_1 = U_1 \cup H = U_1 \cup V_1 = \{y_{11}, y_{12}, \cdots, y_{1h}\}$。

(6)Alice和Bob根据计算原理2 构造$y_{1i} (i = 1, 2, \cdots, h)$在$U, V$中的重数$p_i, q_i$对应的向量$\boldsymbol{S}_i = (s_{i1}, s_{i2}, \cdots, s_{id})^{\mathrm{T}}$和$\boldsymbol{T}_i = (t_{i1}, t_{i2}, \cdots, t_{id})^{\mathrm{T}}$，根据协议2的后续步骤构造$\boldsymbol{S}_i^1, \boldsymbol{S}_i^2$和$\boldsymbol{T}_i^1, \boldsymbol{T}_i^2$，满足$\boldsymbol{S}_i = \boldsymbol{S}_i^1 + \boldsymbol{S}_i^2, \boldsymbol{T}_i = \boldsymbol{T}_i^1 + \boldsymbol{T}_i^2$，计算内积$\boldsymbol{S}_i \cdot \boldsymbol{T}_i = \boldsymbol{S}_i^1 \cdot \boldsymbol{T}_i^1 + \boldsymbol{S}_i^1 \cdot \boldsymbol{T}_i^2 + \boldsymbol{S}_i^2 \cdot \boldsymbol{T}_i^1 + \boldsymbol{S}_i^2 \cdot \boldsymbol{T}_i^2$，则$y_{1i}$的重数$y_{2i} = d - \boldsymbol{S}_i \cdot \boldsymbol{T}_i = \max\{p_i, q_i\}$。

(7)输出两方多重集并集$Y = U \cup V = \{< y_{11}, y_{21} >, < y_{12}, y_{22} >, \cdots, < y_{1h}, y_{2h} >\}$。

$$\boldsymbol{S}_i=\left(\underbrace{0,0,\cdots,0}_{p_i\text{个}1},\underbrace{1,1,,\cdots,1}_{d-p_i\text{个}1}\right)^{\mathrm{T}},$$
$$\boldsymbol{T}_i=\left(\underbrace{0,0,\cdots,0}_{q_i\text{个}0},\underbrace{1,,1\cdots,1}_{d-q_i\text{个}1}\right)^{\mathrm{T}} \tag{18}$$

其中，$0<p_i\le d,0<q_i\le d$。 两人随机生成向量$\boldsymbol{S}_i^1,\boldsymbol{T}_i^1$，再计算$\boldsymbol{S}_i^2,\boldsymbol{T}_i^2$，其中，$\boldsymbol{S}_i^2=\boldsymbol{S}_i-\boldsymbol{S}_i^1$, $\boldsymbol{T}_i^2=\boldsymbol{T}_i-\boldsymbol{T}_i^1$，由命题1得内积$\boldsymbol{S}_i\cdot\boldsymbol{T}_i=\boldsymbol{S}_i^1\cdot\boldsymbol{T}_i^1+\boldsymbol{S}_i^1\cdot\boldsymbol{T}_i^2+\boldsymbol{S}_i^2\cdot\boldsymbol{T}_i^1+\boldsymbol{S}_i^2\cdot\boldsymbol{T}_i^2=\min\{d-p_i,d-q_i\}$，所以元素$y_{1i}$在多重集并集中的重数$y_{2i}=d-\boldsymbol{S}_i\cdot\boldsymbol{T}_i=\max\{p_i,q_i\}$。因此，协议2是正确的。

3.4.3 安全性分析

由于协议2的设计是对协议1部分步骤进行了修改，下面讨论修改后的步骤的安全性。协议第(3)步Alice计算内积$Z_j(j=1,2,\cdots,l)$，得到l维向量$\boldsymbol{E}=(e_1,e_2,\cdots,e_l)$，并选取随机整数$r$，将向量$\boldsymbol{E}$中的$r$个1变为0，得到新的向量$\boldsymbol{E}'$，把$\boldsymbol{E}'$发送给Bob。在这个过程中，Alice通过改变$\boldsymbol{E}$的分量隐藏了自己的集合元素且不影响最终结果的输出，Bob也无法获得Alice私密集合的信息。在第(4)步Bob选取向量$\boldsymbol{E}'$中的前m个分量中0所在位置对应的v_{1j}构成集合H，将集合元素随机置换后发送给Alice, Alice无法从集合H中得到Bob集合的私密信息包括集合的势。第(5)步Alice输出标准集并集$Y_1=U_1\cup V_1$，然后两人调用保密内积协议计算并集元素重数，其安全性可由保密内积协议的安全性保证。在整个协议过程中，双方集合的私密信息都没有任何泄露，因此协议是安全的。

定理2 在半诚实模型下协议2是安全的。

定理2的证明过程与定理1类似，在此省略具体证明过程。

4 性能分析

下面对本文中协议的计算复杂性和通信复杂性进行分析。本文协议设计均基于保密内积协议，适用于有理数多重集，没有使用任何公钥加解密算法，以乘法运算次数计算协议的计算复杂性；文献[16]结合Paillier加密算法设计保密计算协议，适用于整数多重集，需要给定包含所有集合元素的全集，以模指数运算次数计算协议的计算复杂性，其他花费忽略不计，并以协议执行过程中参与者通信的次数来计算通信复杂性。将本文所设计协议与文献[16]中协议的效率和适用性进行比较，结果如表1所示。

其中，M_{p}为Paillier加密方案中的模指数运算，M为乘法运算；文献[16]协议中的s为给定包含两方多重集元素的全集的势，t大于等于两方多重集元素的最大重数。本文协议中的l为Alice和Bob共同协商的整数，满足$l>\max\{n,m\}$，n,m为Alice和Bob所拥有的集合(标准集)的势； $d\ge\max\limits_{1\le i\le n,1\le j\le m}\{u_{2i},v_{2j}\}$, u_{2i},v_{2j}分别为多重集元素u_{1i},v_{1j}的重数；k为多重集标准集的交集的势，h为多重集标准集的并集的势。

本文协议主要使用了乘法运算，由表1可知，协议具有2次计算复杂性。与文献[16]相比，本文协议可以解决有理数域上多重集的计算问题，适用范围更广。

下面对本文协议进行实验测试，实验环境：Windows11家庭中文版，AMD Ryzen 7 5800H with Radeon Graphics @3.20 GHz，安装内存16.0 GB, 64 位操作系统，采用python3.10.4编程语言。

以集合$U=\{<12/5,5>,<3/7,2>,<1/3,7>,<29/17,1>,<68/21,2>,<16,4>,<19/3,3>,<76/15,6>,<8/3,5>,<5/2,6>\}$和$V=\{<3/7,5>,<1/3,4>,<12/5,3>,<9,6>,<61/59,8>,<29/17,7>,<56/13,4>,<15/2,4>,<12/7,2>,<32/7,7>\}$为例对本文协议1,2进行仿真实验，求取100次实验结果平均值，结果如表2所示。

数据预处理是协议的准备工作中Alice和Bob根据各自的私密有理数多重集的标准集得到对应向量的过程。

由表2可知，本文协议1,2计算效率较高。

为了测试本文协议1,2的执行效率与多重集元素重数的关系，固定多重集的标准集不变，改变元素最大重数，时间为交互计算耗时，对协议进行实际计算，分别求取100次实验结果平均值，实验结果如图1。

表 1 协议的效率分析和适用性范围比较

协议	计算功能	计算复杂性	通信复杂性	适用范围
文献[16]协议1	两方多重集交集	$s(t+1)M_{\mathrm{p}}$	3	整数
本文协议1		$[l(3l+4)+4k(3d+1)]M$	7	有理数
文献[16]协议2	两方多重集并集	$s(t+1)M_{\mathrm{p}}$	3	整数
本文协议2		$[l(3l+4)+4h(3d+1)]M$	8	有理数

表 2　实验结果分析(ms)

协议	数据预处理耗时	交互计算耗时	实验总耗时
协议1	38.31	0.73	39.04
协议2	38.65	1.91	40.56

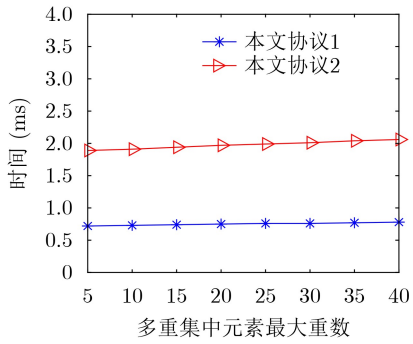

图 1 交互计算耗时随元素重数变化规律

由图1可知，当集合元素固定时，协议1,2的交互计算耗时随多重集中元素最大重数的增长而线性增长。

综合上述分析，与文献[16]相比，本文具有以下优点：

第一，本文提出的多重集的保密计算协议适用于有理数集合，无需给定包含所有集合元素的全集，可以同时保证集合元素和集合势的隐私性。

第二，本文协议计算效率较高，优势明显。本文协议在执行过程中主要使用了乘法运算，当有理数多重集退化为整数多重集时，本文协议所需的乘法运算时间远小于文献[16]的模指数运算时间。

第三，固定集合元素不变时，本文协议的交互计算耗时虽受元素最大重数变化的影响，但其线性增长速度小于文献[16]中的协议。

5　结论

本文通过有理数的几何编码，将有理数域上的集合运算转化为了计算整数向量内积问题，并结合保密内积协议首次设计了有理数域上两方多重集交集和并集的保密计算协议。所设计协议在执行过程主要使用乘法运算，达到了信息论安全，而且无需给定包含所有集合元素的全集，保证了参与者集合元素和集合势的隐私性。在半诚实模型下，应用模拟范例证明了所有协议的安全性，理论分析和仿真实验结果均表明本文协议是高效的。

参 考 文 献

[1] YAO A C. Protocols for secure computations[C]. The 23rd Annual Symposium on Foundations of Computer Science, Chicago, USA, 1982: 160–164. doi: 10.1109/SFCS.1982.38.

[2] TANG Chunming, SHI Guihua, and YAO Zhengan. Secure multi-party computation protocol for sequencing problem[J]. *Science China Information Sciences*, 2011, 54(8): 1654–1662. doi: 10.1007/s11432-011-4272-1.

[3] TOFT T. Sub-linear, secure comparison with two non-colluding parties[C]. The 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, 2011: 174–191. doi: 10.1007/978-3-642-19379-8_11.

[4] LI Shundong, WU Chunying, WANG Daoshun, *et al*. Secure multiparty computation of solid geometric problems and their applications[J]. *Information Sciences*, 2014, 282: 401–413. doi: 10.1016/j.ins.2014.04.004.

[5] 郭奕旻, 周素芳, 窦家维, 等. 高效的区间保密计算及应用[J]. 计算机学报, 2017, 40(7): 1664–1679. doi: 10.11897/SP.J.1016.2017.01664.
GUO Yimin, ZHOU Sufang, DOU Jiawei, *et al*. Efficient privacy-preserving interval computation and its applications[J]. *Chinese Journal of Computers*, 2017, 40(7): 1664–1679. doi: 10.11897/SP.J.1016.2017.01664.

[6] 张卫国, 孙嫚, 陈振华, 等. 空间位置关系的安全多方计算及其应用[J]. 电子与信息学报, 2016, 38(9): 2294–2300. doi: 10.11999/JEIT160102.
ZHANG Weiguo, SUN Man, CHEN Zhenhua, *et al*. Secure multi-party computation of spatial relationship and its application[J]. *Journal of Electronics & Information Technology*, 2016, 38(9): 2294–2300. doi: 10.11999/JEIT160102.

[7] NIKSEFAT S, SADEGHIYAN B, MOHASSEL P, *et al*. ZIDS: A privacy-preserving intrusion detection system using secure two-party computation protocols[J]. *The Computer Journal*, 2014, 57(4): 494–509. doi: 10.1093/comjnl/bxt019.

[8] GRIGORIEV D and SHPILRAIN V. Yao's millionaires' problem and decoy-based public key encryption by classical physics[J]. *International Journal of Foundations of Computer Science*, 2014, 25(4): 409–417. doi: 10.1142/S0129054114400036.

[9] LI Shundong, WANG Daoshun, and DAI Yiqi. Symmetric cryptographic protocols for extended millionaires' problem[J]. *Science in China Series F:Information Sciences*, 2009, 52(6): 974–982. doi: 10.1007/s11432-009-0109-6.

[10] FREEDMAN M J, NISSIM K, and PINKAS B. Efficient private matching and set intersection[C]. International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, 2004: 1–19. doi: 10.1007/978-3-540-24676-3_1.

[11] 陈振华, 李顺东, 黄琼, 等. 非加密方法安全计算两种集合关系[J]. 软件学报, 2018, 29(2): 473–482. doi: 10.13328/j.cnki.jos.005262.
CHEN Zhenhua, LI Shundong, HUANG Qiong, *et al*. Secure computation of two set-relationships with the unencrypted

method[J]. *Journal of Software*, 2018, 29(2): 473–482. doi: 10.13328/j.cnki.jos.005262.

[12] SEO J H, CHEON J H, and KATZ J. Constant-round multi-party private set union using reversed Laurent series[C]. The 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, 2012: 398–412. doi: 10.1007/978-3-642-30057-8_24.

[13] CHUN Jiyong, HONG D, JEONG I R, *et al*. Privacy-preserving disjunctive normal form operations on distributed sets[J]. *Information Sciences*, 2013, 231: 113–122. doi: 10.1016/j.ins.2011.07.003.

[14] KISSNER L and SONG D. Privacy-preserving set operations[C]. The 25th Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, USA, 2005: 241–257. doi: 10.1007/11535218_15.

[15] BLANTON M and AGUIAR E. Private and oblivious set and multiset operations[J]. *International Journal of Information Security*, 2016, 15(5): 493–518. doi: 10.1007/s10207-015-0301-1.

[16] 窦家维, 陈明艳. 多重集的保密计算及应用[J]. 电子学报, 2020, 48(1): 204–208. doi: 10.3969/j.issn.0372-2112.2020.01.025.

DOU Jiawei and CHEN Mingyan. Secure multiset operations and their applications[J]. *Acta Electronica Sinica*, 2020, 48(1): 204–208. doi: 10.3969/j.issn.0372-2112.2020.01.025.

[17] CHUNG H and KIM M. Encoding of rational numbers and their homomorphic computations for FHE-based applications[J]. *International Journal of Foundations of Computer Science*, 2018, 29(6): 1023–1044. doi: 10.1142/S0129054118500193.

[18] 李顺东, 杜润萌, 杨颜璟, 等. 有理数相等的保密判定[J]. 电子学报, 2020, 48(10): 1933–1937. doi: 10.3969/j.issn.0372-2112.2020.10.009.

LI Shundong, DU Runmeng, YANG Yanjing, *et al*. Privately determining equality of rational numbers[J]. *Acta Electronica Sinica*, 2020, 48(10): 1933–1937. doi: 10.3969/j.issn.0372-2112.2020.10.009.

[19] 窦家维, 刘旭红, 王文丽. 有理数域上两方集合的高效保密计算[J]. 计算机学报, 2020, 43(8): 1397–1413. doi: 10.11897/SP.J.1016.2020.01397.

DOU Jiawei, LIU Xuhong, and WANG Wenli. Privacy preserving two-party rational set computation[J]. *Chinese Journal of Computers*, 2020, 43(8): 1397–1413. doi: 10.11897/SP.J.1016.2020.01397.

[20] GOLDREICH O. Foundations of Cryptography Volume 2: Basic Applications[M]. Cambridge: Cambridge University Press, 2004. doi: 10.1017/CBO9780511721656..

[21] REIMER B, FRIED R, MEHLER B, *et al*. Brief report: Examining driving behavior in young adults with high functioning autism spectrum disorders: A pilot study using a driving simulation paradigm[J]. *Journal of Autism and Developmental Disorders*, 2013, 43(9): 2211–2217. doi: 10.1007/s10803-013-1764-4.

[22] CLIFTON C, KANTARCIOGLU M, VAIDYA J, *et al*. Tools for privacy preserving distributed data mining[J]. *ACM SIGKDD Explorations Newsletter*, 2002, 4(2): 28–34. doi: 10.1145/772862.772867.

王维琼：女，博士，教授，研究方向为编码理论与密码学.
谢 琼：女，硕士生，研究方向为密码学.
许豪杰：男，硕士生，研究方向为密码学.
崔 萌：女，硕士生，研究方向为密码学.

责任编辑：余 蓉